

بعض أنماط جرائم الاعتداء على النظم المعلوماتية في المؤسسات

إعـداد
المستشار/ محمد محمد الالفي
رئيس المحكمة
عضو المجموعة التأسيسية للجمعية الدولية لقانون الإنترنت

---

* ورقة عمل مقدمة في ندوة " مكافحة الجريمة عبر الإنترنت على المستوي العربي"، شرم الشيخ – جمهورية مصر العربية، ابريل 2008.

تمهيد:

سنتناول في هذه الورقة النقاط الأتية:

- مقدمة.
- جريمة قرصنة برامج الحاسوبية عبر شبكة الإنترنت.
- ماهية جرائم قرصنة البرامج الحاسوبية.
- جريمة إتلاف وتدمير المعطيات والبيانات والنظم المعلوماتية.
- الماهية القانونية لجرائم الإتلاف في المجال المعلوماتي والكيفية التي تتم بها.
- صور الاعتداء على المكونات المنطقية للحاسب الآلي:

1. الإدخال غير المشروع للمعلوماتIntroduction
2. تدمير البيانات والمعلوماتDestruction
3. التعديل غير المشروع للمعلومات والبياناتModification

مقدمة:

أمن المعلومات، من زاوية اكاديمية، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها . ومن زاوية تقنية، هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية . ومن زاوية قانونية، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت) .

واستخدام اصطلاح أمن المعلومات Information Security وان كان استخداما قديما سابقا لولادة وسائل تكنولوجيا المعلومات، الا انه وجد استخدامه الشائع بل والفعلي، في نطاق انشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال، اذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات- وتحديدا الإنترنت – احتلت ابحاث ودراسات أمن

المعلـــومات مـــساحة رحـــبة آخـــذة فـــي النماء من بين أبحاث تقنية المعلومات المختلفة، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات .

ان الارقـــام قـــد تغنـــي عـــن الكثيـــر مـــن الأقوال، واحيانا عن ايجاد مدخل مناسب للحـــديث عـــندما تتـــزاحم العقـــل افكـــار عديـــدة ، ففي احدث تقارير مركز شكاوى احتيال الإنتـــرنت (IFFC) الأمريكـــي، اظهـــر التحلـــيل الـــشامل للـــشكاوى التي قدمت للمركز، ان عـــدد الـــشكاوى التـــي تلقاهـــا المركـــز مـــنذ بدأ اعماله في ايار 2000 وحتى شهر تشرين ثانـــي مـــن نفـــس العـــام (اي خـــلال ســـتة اشهر فقط) قد بلغت 6087 شكوى، من ضمنها 5273 حالـــة تـــتعلق باختـــراق الكمبيوتـــر عبـــر الإنتـــرنت و814 تـــتعلق بوسائل الدخول والاقـــتحام الاخـــرى كالدخـــول عبـــر الهاتـــف او الدخـــول المباشر الى النظام بشكل مادي، مـــع الاشـــارة الـــى ان هـــذه الحـــالات هـــي فقـــط التـــي تم الابلاغ عنها ولا تمثل الارقام الحقيقـــية لعـــدد حـــالات الاحتـــيال الفعلـــي، وهي تتعلق فقط بجريمة الاحتيال عبر الإنترنت التـــي هـــي واحـــدة مـــن العديـــد من انماط جرائم الكمبيوتر والإنترنت . وقد بلغت الخسائر المتـــصلة بهـــذه الـــشكاوى مـــا يقـــارب 4.6 ملـــيون دولار وهـــي تقارب 33% من حجم الخـــسائر الناشـــئة عـــن كافـــة جرائم الاحتيال التقليدية المرتكبة في نفس الفترة . وان 22% مـــن هـــذه الخـــسائر نجمـــت عـــن شراء منتجات عبر الإنترنت دون ان يتم تسليم البضاعة فعليا للمشترين، وان 5% منها نشأت عن احتيال بطاقات الائتمان .

ان ظاهـــرة جـــرائم الكمبيوتـــر والانتـــرنت، او جـــرائم التقنـــية العالية، او الجريمة الإلكتـــرونية، او (الـــسيبر كـــرايم- Cyber Crime)، او جـــرائم اصـــحاب الياقات البيضاء White Collar، ظاهـــرة اجـــرامية مـــستجدة نـــسبيا تقـــرع في جنباتها أجراس الخطر لتنبه مجـــتمعات العـــصر الـــراهن لحجـــم المخاطـــر وهـــول الخـــسائر الناجمة عنها، باعتبارها تـــستهدف الاعـــتداء علـــى المعطـــيات بدلالـــتها التقنية الواسعة، (بيانات ومعلومات وبرامج بكافـــة أنـــواعها). فهـــي جـــريمة تقنـــية تنـــشأ في الخفاء يقارفها مجرمون أذكياء يمتلكون أدوات المعـــرفة التقنـــية، تـــوجه للنـــيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الكمبيوتـــر المخـــزنة والمعلـــومات المـــنقولة عبـــر نظـــم وشبكات المعلومات وفي مقدمتها الإنتـــرنت . هـــذه المعطـــيات هـــي موضـــوع هـــذه الجريمة وما تستهدفه اعتداءات الجناة، وهـــذا وحـــده - عبـــر دلالـــته العامـــة - يظهـــر مدى خطورة جرائم الكمبيوتر، فهي تطال الحـــق فـــي المعلـــومات، وتمـــس الحـــياة الخاصـــة للأفـــراد وتهـــدد الأمن القومي والسيادة

الوطنـــية وتـــشيع فقـــدان الـــثقة بالتقنـــية وتهـــدد ابـــداع العقل البشري. لذا فان ادراك ماهية جـــرائم الكمبيوتـــر والانتـــرنت، والطبـــيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجم عنها وسمات مرتكبيها ودوافعهم

أن جـــريمة الكمبيوتـــر تـــتحقق باســـتخدام الكمبيوتـــر وسيلة لارتكاب الجريمة، من هـــذه التعـــريفات، يعـــرفها الأســـتاذ جـــون فورستر [1] وكذلك الأستاذ Eslie D. Ball أنهـــا "فعـــل اجرامـــي يـــستخدم الكمبيوتـــر فـــي ارتكابـــه كـــأداة رئيـــسية" ويعـــرفها تاديمـــان Tiedemaun بأنهـــا "كـــل أشـــكال الـــسلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكـــذلك يعـــرفها مكـــتب تقيـــيم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيساً" [2]

جانـــب مـــن الفقـــه والمؤســـسات ذات العلاقـــة بهـــذا الموضوع، وضعت عددا من التعـــريفات التـــي تقـــوم علـــى اســـاس سمات شخصية لدى مرتكب الفعل، وهي تحديدا سمة الدرايـــة والمعـــرفة التقنـــية . مـــن هـــذه التعـــريفات، تعـــريف وزارة العدل الأمريكية في دراســـة وضـــعها معهـــد ســـتانفورد للابحـــاث وتبنـــتها الوزارة في دليلها لعام 1979، حيث عـــرفت بانهـــا " ايـــة جـــريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها" . ومن هذه التعـــريفات أيـــضا تعـــريف David Thompson بانهـــا " اية جريمة يكون متطلبا لاقترافها ان تتوافـــر لـــدى فاعلهـــا معـــرفة بتقنية الحاسب". وتعريـــف Stein Schjqlberg بانهـــا " أي فعـــل غيـــر مـــشروع تكـــون المعـــرفة بتقنـــية الكمبيوتر اساسية لارتكابه والتحقيق فيه وملاحقته قضائيا " [3]

كمـــا يعـــرفها الأســـتاذ ldon. J. HechteSh بأنهـــا: "واقعـــة تتضمن تقنية الحاسب ومجنـــي علـــيه يتكـــبد أو يمكـــن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول علـــى مكـــسب" وقـــريب مـــنه تعـــريف الفقـــيه Parker Bdonn . فـــي مـــؤلفه Fighting rimeCComputer والـــذي يـــرى بأنهـــا "أي فعـــل مـــتعمد مـــرتبط بأي وجه، بالحاسبات، يتـــسبب فـــي تكـــبد أو امكانـــية تكـــبد مجنـــي علـــيه لخسارة أو حصول أو امكانية حصول مرتكبه على مكسب" ويستخدم للدلالة على الجريمة تعبير "إساءة استخدام الحاسوب".

---

(1) Tom forester, Essential problems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, P. 104

(2) مشار إلى هذه التعريفات لدى د. رستم، السابق، ص 29 و30 .

(3) انظر، د. رستم، السابق، ص 32 .

وقد عرف جريمة الكمبيوتر خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD، بانها " كل فعل او امتناع من شانه الاعتداء على الأمواج المادية او المعنوية يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية "[1].

والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين [2] بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الاحاطة الشاملة قدر الامكان بظاهرة جرائم التقنية، ولأن التعريف المذكور يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، ولأنه أخيرا يتيح امكانية التعامل مع التطورات المستقبلية التقنية.

ان الجرائم التي تطال ماديات الكمبيوتر ووسائل الاتصال، شأنها شأن الجرائم المستقرة على مدى قرنين من التشريع الجنائي، محلها أموال مادية صيغت على أساس صفتها نظريات وقواعد ونصوص القانون الجنائي على عكس (معنويات) الكمبيوتر ووسائل تقنية المعلومات، التي أفرزت أنشطة الاعتداء عليها تساؤلا عريضا – تكاد تنحسم الاجابة عليه بالنفي- حول مدى انطباق نصوص القانون الجنائي التقليدية عليه.

ويعرف خبراء منظمة التعاون الاقتصادي والتنمية، جريمة الكمبيوتر بأنها :

"كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/ أو نقلها" [3]

(1) www.oecd.org

(2) د. رستم، السابق، ص 35 .

(3) انظر موقع المنظمة على شبكة الانترنت – مشار إليه فيما سبق .

جريمة قرصنة برامج الحاسوبية عبر شبكة الإنترنت:

تمهيد وتقسيم:

مع بزوغ عصر الثورة المعلوماتية ظهرت لأول مرة في تاريخ البشرية مشكلة التعامل مع شكل جديد من أشكال الملكيات تسمي الملكيات الرقمية ويقصد بها "البرمجيات الحاسوبية وبياناتها"(1).

فهي نمط جديد من أوعية المعرفة لها خصوصياتها وتحتاج لمعاملة خاصة، وأهم ما يميزها تكاليفها الباهضة بالنظر إلى سهولة تداولها واستنساخها خاصة مع ظهور شبكة الإنترنت.

وبالتالي ظهرت على الساحة جرائم هي في الأساس ذات أصل تقليدي، لكن وبفضل التطور الكبير في تكنولوجيا المعلومات وشبكات الاتصال أصبحت مستحدثة وذلك بالنظر إلى محلها، ألا وهي جرائم قرصنة(2) برامج الحاسب الآلي عبر شبكة الإنترنت .

ودراستنا لهذا النوع من الجرائم سوف يكون من خلال محورين اثنين الأول يبحث الماهية القانونية لهذه الجرائم والكيفية التي تتم بها، في حين أن الثاني يبحث الموقف الإسلامي منها. وسوف نخصص لكل محور فرعا خاصا به .

---

(1) د.م.عارف الطرابيشى : مستجدات حقوق الملكية الفكرية في تقانات المعلومات وصناعة البرمجيات الحاسوبية، بحث مقدم إلى ندوة آفاق الملكية الفكرية في عصر المعلومات والتي عقدت بالتعاون بين اللجنة العربية لحماية الملكية الفكرية مع اللجنة التحضيرية لإتحاد الناشرين السوريين بالجمهورية العربية السورية 2000/10/10م.، منشور على شبكة الإنترنت من خلال:
www.arabpip.org/lecturress-nl-3htm.

(2) كلمة قرصنة تعني في أصلها ومعناها الدقيق كل عمل عنيف غير مرخص به يرتكب بقصد النهب من قبل سفينة خاصة ضد سفينة أخرى في أعالي البحار، ومنذ أوائل القرن الثامن عشر أصبحت وصفا يطلق من باب القياس والاستهجان على نهب المصنفات المنشورة للغير بنسخها دون ترخيص بقصد الاتجار، ومن هذا المنطلق شاع استخدام تعبير قرصنة البرامج . أنظر د. محمد السعيد رشدي : الإنترنت والجوانب القانونية لنظم المعلومات، دار النهضة العربية، القاهرة 2004م ص 31.

الفرع الأول
ماهية جرائم قرصنة البرامج الحاسوبية

برامج الحاسب الآلي تشكل الكيان المعنوي أو المنطقي لنظام الحاسب الآلي فبدونها لا تكون ثمة فائدة للمكونات المادية لجهاز الحاسب الآلي . ويمكن تعريفها بأنها: " مجموعة العبارات والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة والمعدة للاستعمال في الحاسب الآلي بطريق مباشر أو غير مباشر بهدف التوصل إلى نتائج محددة"[1].

وهي تنقسم من الناحية التقنية إلى نوعين: برمجيات التشغيل ويناط بها مسؤولية عمل مكونات النظام معا وتوفير بيئة مناسبة لعمل النوع الثاني من البرمجيات وهي البرمجيات التطبيقية، وهذه الأخيرة عديدة وتختلف فيما بينها باختلاف المهمة التي تقوم بها، منها على سبيل المثال برامج معالجة النصوص وبرامج الجداول أو الرسوم والبرامج التعليمية وغيرها من البرامج[2].

أما من ناحية الدراسات التشريعية والقانونية فقد ظهرت العديد من المفاهيم المتصلة بأنواع البرامج أبرزها برامج المصدر وبرامج الآلة والخوارزميات ولغات البرمجة وبرامج الترجمة[3].

والهدف من إصباغ الحماية الجنائية على برامج الحاسب الآلي الرغبة في تشجيع الناس إلى ابتكار البرامج التي من شأنها المساهمة وبشكل كبير في إثراء الدول وتقدمها، وتحقيق أهداف التنمية الاقتصادية بها، بالإضافة إلى أن هذه الحماية تحول دون تفاقم مشكلة القرصنة الدولية لهذه البرامج الحاسوبيه ويقصد بها عملية النسخ غير المشروع أو الاستخدام غير المرخص به لبرامج الغير والتي أصبحت وبحق من أهم العقبات التي تواجه مستقبل الصناعات المعلوماتية، حيث تتكبد الشركات العاملة في هذا المجال مليارات الدولارات سنويا[4].

---

(1) المادة الأولى من قانون حماية حقوق المؤلف والحقوق المجاورة الصادرة بالمرسوم السلطاني رقم37/2000.

(2) د. يونس عرب: الملكية الفكرية للمصنفات الرقمية، دراسة منشورة على شبكة الإنترنت من خلال: www.arablaw.net ص2.

(3) محمد محمد شتا: فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية 2001 ص 64.

(4) أسباب تفاقم هذه المشكلة يرجع إلى غلاء أسعار برامج الحاسب الآلي الأصلية مقارنة بالبرامج المنسوخة، وبالتالي فإن الإقبال على هذه الأخيرة أصبح كبيرا وذلك لرخص ثمنها فهي في متناول الجميع، حيث أن

ففـــي إحـــصائية حديـــثة قامـــت بهـــا مـــنظمة إتحاد صناعة البرمجيات والمعلومات SIIA، قـــدرت الخـــسائر التـــي تـــسببت بهـــا القرصـــنة العالمـــية في مجال البرمجيات فقط بحوالـــي 11ملـــيار دولار أمريكـــي[1]!!، وفـــي دراســـة قام بها مجلس الشيوخ الأمريكي مع بدايـــة الألفـــية الجديـــدة وجـــد أن العـــدوان علـــى برامج الحاسب الآلي في الولايات المتحدة يـــشكل مـــا نـــسبته 27%مـــن حـــركة تداول البرامج الحاسوبية في السوق الأمريكية، وتصل إلـــى 90% فـــي أســـواق أخـــري[2]. مـــن أجـــل ذلك طالبت الدول المنتجة والمصدرة لهذه البـــرامج الـــدول المـــستهلكة مباشـــرة بـــضرورة قيام هذه الأخيرة بسن التشريعات والقوانين التي تكفل لهذه البرامج الحماية اللازمة من العدوان عليها[3].

مواقـــع الـــويب علـــى شـــبكة الإنتـــرنت حيث يتم نشر الإصدارات الحديثة منها في مواقع القرصنة قبل وصول النسخ الأصلية منها إلى الأسواق[4].

ومـــن ناحـــية أخـــرى نجـــد الكثيـــر من برامج الحاسب الآلي التي توزع على شبكة الإنتـــرنت، إمـــا مجانـــية وتـــسمي بالبـــرامج المجانـــية Free Ware [5] وإما بشكل تشاركي وتـــسمي بالبـــرامج المتـــشاركة Shareware[6] . وهـــنا يُـــثار التساؤل حول الوضع القانوني لها هل تعتبر حرة من الحقوق مما يعني حرية الوصول إليها؟

عملية النسخ عملية سهلة جدا بعد أن يتم كسر حمايتها، بالإضافة إلى نقص الوازع الديني لدى الناس وحبهم للكسب السريع، كما يعد عدم وجود نظام صارم لمكافحة هذه الجريمة أو عدم وجود صرامة وجدية في تطبيق العقوبات يساعد على تفاقم هذه الظاهرة : حول هذا الموضوع أنظر: محسن بن سليمان خليفة: جرائم الحاسب الآلي وعقوبتها في الفقه والنظام، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا،الرياض 1423هـ - 1424هـ ص 107-109.

(1) www.siia.net/news/releases/p..obalpiracy.htm

(2) د. عمر محمد أبو بكر بن يونس – الجرائم الناشئة عن استخدام الإنترنت – المرجع السابق ص 545.

(3) من الأمثلة على ذلك قيام الولايات المتحدة في مارس 2001 بمطالبة مملكة تايون بضرورة استصدار تشريع خاص لمكافحة قرصنة البرامج سواء من حيث مراقبة حركتها وتصديرها واستيرادها وملكيتها. ونسخها.

(4) على سبيل المثال : لعبة Halflife التي تنتشر في مواقع warez ومواقع الدردشة IRC كانتشار النار في الهشيم قبل أن تطرحها الشركة المنتجة في الأسواق المحلية على الرغم من أن حجم ملفاتها كان كبيرا جدا يصل إلى 250ميجا بايت www.arabiyat.com/forums/archive/topic/27905-1.html.

(5) يقصد بالبرامج المجانية : البرامج التي تمنح حقوق استعمالها واستغلالها إلى الغير مجانا. أنظر. ديالا عيسى ونسه: حماية حقوق التأليف على شبكة الإنترنت " دراسة مقارنة"، صادر ناشرون، لبنان 2002م ص186.

(6) يقصد بالبرامج التشاركية البرامج الموضوعة تحت تصرف من يشاء من الجمهور (داخل الشبكة أو خارجها) لقاء تعويض، لا يجبر من قام باستعمالها على الدفع، إلا إذا رضي عنها تجربتها مدة من الزمن.أنظر. ديالا عيسى ونسه : المرجع السابق ص 187.

ومـــن أشـــهر الطـــرق التـــي تـــتم بهـــا عملية قرصنة البرامج الحاسوبية عبر شبكة الإنترنت:

1- **الإنـــزال والتحمـــيل Download** ويتـــضمن إنـــزال برنامج ما أو جزء منه تم تحميله من موقـــع مـــا عبـــر شـــبكة الإنتـــرنت بقصد الاستخدام الخاص ثم يستخدم بعد ذلك تجاريا سواء عن طريق شبكة الإنترنت أو عن طريق الطرق التقليدية في العالم المادي.

2- **العـــرض عبـــر شـــبكة الإنتـــرنت:** هـــذه الصورة تتمثل في قيام الجاني بنسخ برنامج ما مبتكـــر ومعـــد للـــتداول بطـــرق تقلـــيدية معتادة كأن يكون على CD أو Floppy Disk، ومـــن ثـــم رفعهـــا علـــى شـــبكة الإنترنت Upload[1] سواء بهدف العرض المجاني لهذا البـــرنامج أو بهـــدف تـــسويقه وبـــيعه عبـــر بعض المواقع المنتشرة على شبكة الإنترنت والمتخصصة في بيع هذه البرامج المقرصنة.

3- **التـــسويق عبـــر شـــبكة الإنتـــرنت:** تتمـــثل هـــذه الصورة في قيام بعض المحنكين ذوى الخبـــرة العالـــية فـــي كيفـــية فك شفرة البرامج المشفرة ضد عمليات القرصنة والموجودة علـــى شـــبكة الإنتـــرنت ومـــن ثم بيعها عبر بعض المواقع على شبكة الإنترنت، محققين بذلك مكاسب خيالية .

4- **النـــشر عبـــر شـــبكة الإنتـــرنت:** هـــذه الطـــريقة كسابقاتها، إلا أنها تختلف في الغرض فالأولـــى كانـــت بهـــدف الـــربح المادي، أما هنا فإن الهدف هو إتاحة البرنامج للجمهور من خلال شبكة الإنترنت .مما يعني إلحاق الضرر بمنتجي هذه البرامج.

5- **الاعـــتداء علـــى أمـــن حمايـــة التقنـــية:** غالبا ما يعمد مصممو البرامج لأجل تنظيم أو تقـــيد إطـــلاع الجمهـــور علـــى بـــرامجهم إلى استخدام تقنية خاصة عادة ما يطلق عليها "أمن حماية التقنية"[2].

---

(1) يقصد بعملية upload : معالجة إلكترونية تجعل من الممكن استنساخ ملف حاسوبي وإرساله إلى شبكة الإنترنت، عن طريق السماح بتفاعل الغير معه، في حين يظل الملف الأصلي في جهاز الحاسب الآلي الذي وضع فيه هذا الملف، وليتم هذا التداول على شبكة الإنترنت فإنه يلزم أن يكون قد جلب له من قبل جهاز أخر The Receiving Computer.

(2) من هذه الوسائل التشفير واستخدام كلمات السر أو مفاتيح إلكترونية.

ومــع ذلــك يعمــد بعــض الأشــخاص وهــم غالــبا ما يكونون من المحنكين ذوى المهــارة الفائقــة فــي مــسائل التقنــية بإزالــة هــذه التقنية[1] أو تعطيلها[2] أو تعييبها بحيث تــصبح غيــر صــالحة وغيــر فعّالــة وعــندها تــصبح هذه البرامج متاحة للجميع وبالتالي الإضرار بحقوق مؤلفيها ومصمميها.

جريمة إتلاف وتدمير المعطيات والبيانات والنظم المعلوماتية:

تمهيد وتقسيم:

الإتــلاف هــو تخــريب الــشيء محــل الجــريمة بإتلافه أو التقليل من قيمته وذلك بجعلــه غيــر صــالح للاســتعمال أو تعطــيله[3]. وبمعنى أخر تعييب الشيء على نحو يفقده قيمــته الكلــية أو الجــزئية[4]. فهــو إفــناء لمادة الشيء أو على الأقل إحداث تغيرات شاملة علــيها، بحــيث يكــون غيــر صــالح إطلاقا للاستعمال في الغرض المخصص له، ومن ثم تضيع قيمته على المالك.

وانطلاقــا مــع موضــوع الدراســة فــسوف نتــناول فــي هذا المبحث الإتلاف في المجــال المعلوماتــي . وســوف يكــون ذلــك مــن خــلال محــورين اثنين : الأول يتعلق بالماهــية القانونــية لهــذا الــنوع مــن الإتــلاف، والثاني يتعلق بالموقف الإسلامي ي منه. وسوف نخصص لكل محور فرعا مستقلا به.

الفرع الأول
الماهية القانونية لجرائم الإتلاف في المجال المعلوماتي والكيفية التي تتم بها

الإتــلاف فــي المجــال المعلوماتــي قد يقع على المكونات المادية المتصلة بالحاسب الآلــي وملحقاتــه كالــشاشة أو لــوحة المفاتيح أو الفارة أو الأشرطة أو الأقراص الممغنطة وغيــرها ممــا لــه علاقــة بهــذا المجــال . وهــنا يسمى إتلافا ماديا ولا توجد أية عقبات قانونــية تحــول دون تطبــيق النــصوص التقلــيدية الخاصة بجريمة الإتلاف على هذا النوع

---

(1) يقصد بها أي عمل من شأنه أن يؤدي إلى فك هذه الحماية وإزالتها.

(2) يقصد بها أي عمل أو سلوك بأي طريقة كانت من شأنها أن تؤدي إلى عدم تمكين هذه الحماية التقنية من أداء وظيفتها.

(3) محمد عبيد الكعبي : المرجع السابق ص 200.

(4) د.عبد الفتاح بيومي حجازي : التنظيم القانوني لحماية التجارة الإلكترونية "ج2"، دار الفكر الجامعي، الإسكندرية 2002 ص 255.

من الإتلافات على اعتبار أن محل الجريمة مال مادي منقول مملوك للغير، ذلك ان جميع النصوص التي تناولت بيان أحكام جريمة الإتلاف في التشريعات المختلفة تجرم إتلاف المنقولات، فعلى سبيل المثال تجرّم المادة 308 من قانون الجزاء العماني التخريب والإتلاف الذي يقع على أبنية الغير أو على مركباتهم البرية أو المائية او الهوائية، وكذلك تجرّم المادة 311 من ذات القانون التخريب والإتلاف الذي يقع على الآلات والمعدات الزراعية. وذات الشيء نجده في التشريع المصري حيث تجرّم المادة 361من قانون العقوبات المصري التخريب والإتلاف الواقع على المال الثابت أو المنقولات، ونفس الشيء نجده لدى المشرّع الإماراتي من خلال المادة 424 من قانون العقوبات الاتحادي، والفقرة الأولى من المادة 322من قانون العقوبات الفرنسي التي جرمت أفعال التخريب والإتلاف الواقع على المنقولات والعقارات.

الطرق الفنية لإتلاف المكونات المنطقية للحاسب الآلي: تتنوع الطرق الفنية والتقنية المستخدمة في إتلاف المعلومات والبيانات والبرامج والتي تشكل في مجملها المكونات المنطقية للحاسب الآلي. إلا أن أخطرها على الإطلاق استخدام الشفرة الخبيثة Malicious Software : وهي برمجيات ضارة[1] Harmful Rograms وتعد من أخطر العناصر التي تهدد أمن المعلومات والبيانات لأنها تؤدي إلى فقد النظام أو فقد تكامله أو تؤثر على كفاءة أدائه، كما تؤدى إلى إتلاف البرامج وضياع المعلومات . هذا وهي مصممة لتنتقل من حاسب آلي إلى آخر ومن شبكة إلى أخرى بهدف إجراء تعديلات في أنظمة الحاسوب عمدا[2] وبدون موافقة مالكي أو مشغلي هذه الأنظمة .

ويوجد من هذه البرمجيات الكثير حاليا، كما أنه صدر منها العديد في أنحاء متفرقة من العالم، حيث بلغ عددها حتى شهر مايو 2004م 67496 وذلك حسب ما أورده موقع شركة سمانتك المتخصصة في مكافحتها[3].

---

(1) M.Jaugleux Philippe: le crimin alite Dans le erespace (Memoire) fac.des drait des sciences politiques d'Aix – Marseiue.fr.1999 disponible enligne en juin2000 a: www.juriscom.net .p 28.

(2) Susan W–State cyber crime investigation procedure- uni .of Bayton School of law, available in http://cubercrimes.net/Mccip/Mccip.html in Oct. 2001.

(3) محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت " دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية "، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2004م ص 39.

ويمكن تقسيم هذه البرمجيات إلى عدة فئات على النحو التالي:

اولا : الفيروسات Virus :

من المؤكد أن أكثر جرائم الحاسب الآلي إمعانا في الشر هي جريمة النشر الفيروسي، فمن ينشر هذه الفيروسات ينشرها وهو لا يدري من سيصيب؟ وما هي حجم الأضرار التي ستصيب الضحايا ؟.

والفيروسات عبارة عن برمجيات مشفرة للحاسب الآلي مثل أي برمجيات أخرى يتم تصميمها بهدف محدد وهو إحداث أكبر ضرر ممكن بأنظمة الحاسب الآلي، وتتميز بقدرتها على ربط نفسها بالبرامج الأخرى وإعادة إنشاء نفسها حتى تبدوا وكأنها تتكاثر وتتوالد ذاتيا، بالإضافة إلى قدرتها على الانتشار من نظام إلى أخر، أما بواسطة قرص ممغنط أو عبر شبكة الاتصالات بحيث يمكنها أن تنتقل عبر الحدود من أي مكان إلى أخر في العالم .

وعادة ما تسمي باسم أول مكان تكتشف فيه[1] أو باسم مصممها. أي إن الفيروس عبارة عن برنامج يتميز بثلاث خواص هي التضاعف، التخفي، إلحاق الأذى بالآخرين. ويتمثل النشاط التدميري لها في أنها تقوم بمسح البيانات والمعلومات المخزنة على وسائط التخزين وإتلافها لذا يطلق على هذه العملية اسم مسح البيانات وتحويلها إلى صفر ZEROING[2] .

---

(1) للاستزادة حول هذا الموضوع ارجع :

- د.عبادة أحمد عبادة : التدمير المتعمد لأنظمة المعلومات الإلكترونية، بحث منشور لدي مركز البحوث والدراسات، الإدارة العامة لشرطة دبي، مارس 1999 ص1 .
- د. نائلة عادل محمد فريد : المرجع السابق ص 191.
- حسن طاهر داود : أمن شبكات المعلومات، مركز البحوث بمعهد الإدارة العامة بالمملكة العربية السعودية، الرياض 2004ص166.
- د. نادية أمين محمد على: الفيروسات وطرق الوقاية منها كوسيلة لأمن المعلومات، ورقة عمل مقدمة إلى المؤتمر الدولي لأمن المعلومات الإلكترونية"معا نحو تعامل رقمي آمن"، المنعقد في الفترة من 18 -20 ديسمبر 2005م، مسقط، سلطنة عمان.
- Fish Nigri (Dcborah) : National and International aspects of computer crime: the merging need for statutory controls, Thesis .University Of London .Center for criminal law studies, Queen Mary and Westfreld College, January 1993.p189.
- Brenton Chris : Mastering Network Security ,SYBEX ,Network Press, USA, 1999.
- Bentley Tom R: Safe Computing , Untechnical Press, CA, USA, 2000 .
- Gnosh Anup K: Security & Privacy for e-business , John Wiley, USA, 2001.

(2) د. عبادة أحمد عبادة : المرجع السابق ص 21.

أما من حيث الأضرار التي تحدثها بأنظمة الحاسب الآلي فهي تنقسم إلى [1]:

1- الفيروسات التي تصيب الملفات التنفيذية: يقصد بالملفات التنفيذية تلك الملفات التي تكون من نوع EXE، COM، BAT، حيث أن تلك الملفات هي المسئولة عن تشغيل البرامج الموجودة على الحاسب وبالتالي فإن إصابة هذه الملفات يؤدي إلى تعطيل البرنامج بالكامل - خاصة النوع الأول والثاني، أما النوع الثالث فيكاد يكون غير مستخدم في نظم التشغيل الحالية - وبرنامج الفيروس عندما يصيب هذه الملفات فإنه إما أن يقوم بحذف الجزء الأول من الملف التنفيذي وكتابة نفسه في هذا المكان، الأمر الذي يؤدي إلي توقف عمل الملف التنفيذي بشكل جزئي ويعرف هذا النوع من الفيروسات باسم فيروسات الكتابة الفوقية Over Writing Viruses. وإما أن يقوم برنامج الفيروس بنسخ نفسه في الجزء الأخير من الملف التنفيذي وبالتالي فإن الملف التنفيذي يظل يعمل بشكل طبيعي حتى ينشط الفيروس ويقوم بمهامه التخريبية، ويعرف هذا النوع من الفيروسات باسم فيروسات الكتابة غير الفوقيةNon Over Writing Viruses .

2- فيروسات الكتابة المباشرة: وهذا النوع من الفيروسات لا يقوم بنسخ نفسه في ملف عادي مثل النوع الأول، وإنما يقوم بكتابة نفسه مباشرة على الأسطوانة الصلبة في مكان محدد يسمي Boot Record Area وهذا المكان يحتوي على مجموعة من البيانات التي يقوم نظام التشغيل بكتابتها علي القرص الصلب والتي تسمي FAT أو بمعنى آخر فإن هذا النوع من الفيروسات عندما يصيب الحاسب فإنه يؤدي إلي عدم قدرة نظام التشغيل على التعامل مع الملفات بالرغم من أن هذه الملفات مازالت موجودة علي القرص الصلب ولم يتم حذفها ومن أشهر هذه الفيروسات فيروس تشرنوبل.

3- الفيروسات الصغيرة Macro Viruses وهي من الفيروسات الشائعة وتأثيرها ينصب على برامج معالجة النصوص حيث تقوم بإدخال كلمات وعبارات وجمل غير مرغوب فيها وغير متوقعة، وهو غالبا ما يقوم بتعديل الأمر "حفظ" ليشغل نفسه بعد ذلك تلقائيا، وقد تصيب أيضا الملفات الخاص بمستندات النصوص

(1) د. نادية أمين محمد على: المرجع السابق ص5-6.

النشطة HTML المحتوية على نصوص جافا وأنواع أخرى من الرموز التنفيذية، مما يؤدي إلى انتشارها، ومن الأمثلة على هذه الفيروسات فيروس ميليسا الذي ظهر 1999 والذي انتشر عبر البريد الإلكتروني Out Lock.

ثانيا برامج الدودة Worm Software :

هي عبارة عن برامج تقوم باستغلال أية فجوة في أنظمة التشغيل لكي تنتقل من حاسب لآخر، أو من شبكة لأخرى عبر الوصلات التي ترتبط بها وذلك دون حاجة إلى تدخل إنساني لتنشيطها وهذا هو الاختلاف بينها وبين حصان طروادة الذي دائما ما يعتمد على التدخل الإنساني لمباشرة نشاطه كما سنرى لاحقا، كذلك هي لا تلتصق بأنظمة التشغيل في أجهزة الحاسب الآلي التي تصيبها مثلما تفعل الفيروسات[1] كما رينا . وتتكاثر هذه البرامج أثناء عملية انتقالها بإنتاج نسخ منها ودونما الحاجة إلى برامج وسيطة تساعدها على التكاثر[2]، وتعمل على تقليل كفاءة الشبكة أو التخريب الفعلي للملفات والبرامج ونظم التشغيل[3].

ثالثا: حصان طروادة[4] Trojan Horse :

هي عبارة عن برامج فيروسية لديها القدرة على الاختفاء داخل برامج أخرى أصلية للمستخدم بحيث عندما تعمل البرامج الأصلية ينشط الفيروس وينتشر ليبدأ أعماله التخريبية، وهو يختلف عن الفيروس في أنه لا يتكاثر ولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته يحمل في طياته توقيت وأسلوب استيقاظه، وهو يؤدي إلى تعديل هذه البرامج وتزوير المعلومات ومحو بعضها . وقد يصل الأمر إلى تدمير النظام بأكمله[5].

---

(1) د. عمر محمد أبو بكر بن يونس – الجرائم الناشئة عن استخدام الإنترنت – المرجع السابق 367.

(2) محمد عبيد الكعبي – الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، رسالة ماجستير، كلية الحقوق جامعة القاهرة 2004 ص 217.

(3) محمد أمين أحمد الشوابكة جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن 2004 ص 240.

(4) أصل التسمية يرجع إلى حصان طروادة الذي استخدمه الإغريق في اختراق حصن طروادة، عندما تعذر عليهم دخول حصن طروادة المنيع فما كان منهم إلا أن صنعوا هيكل حصان ووضعوا فيه جنود من الإغريق وانسحبوا من ميدان القتال موهمين قوات طروادة أنهم عجزوا عن مواصلة دخول الحصن ومواصلة الحصار تاركين هيكل الحصان خلفهم، عندها فرحت قوات طروادة بالحصان وأخذه معهم إلى داخل الحصن، وفي الليل خرج الجنود الإغريق من الحصان وفتحوا أبواب الحصن فدخلت القوات الإغريقية.

(5) د. هدي حامد قشقوش: المرجع السابق ص 103.

رابعا: القنبلة المعلوماتية Bomb :

هــي نــوع مــن البــرامج الخبيــثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفــية مــع بــرامج أخــرى . فــشكليا هي ليست ملفا كاملا متكاملا وإنما شفرة تنضم إلى مجمــوعة ملفــات البــرامج وذلــك بتقــسيمها إلــى أجزاء متفرقة هنا وهناك حتى لا يمكن التعــرف علــيها بحــيث تــتجمع فــيما بيــنها بحــسب الأمر المعطى لها في زمن معين أو حــدوث واقعــة معيــنة، فهــي مــصممة بحيث تبقي ساكنة وغير فعالة إلا في الزمن المحدد أو الــواقعة المحــددة لــذا يــتعذر اكتشافها لمدة قد تصل لأشهر وأعوام(1)، ويؤدي اجتماعها هــذا إلــى انعــدام القــدرة علــى تشغيل البرنامج عبر جهاز الحاسب الآلي(2). وتستخدم هذه البــرامج لإتــلاف المعلــومات والبــيانات وتغييــر بــرامج ومعلــومات النظام.وقد تستخدم كبــرامج لحمايــة الملكــية الفكــرية مــن القرصــنة وخاصــة تلــك التي تحدث عبر شبكة الإنتــرنت، فالــذي يملــك حقــوق النسخ قد يجيز للغير نسخ مصنفه عبر شبكة الإنترنت إلا أن هــذه الإجــازة قــد تكــون لفتــرة محــددة بفترة زمنية قصيرة تختفي بعدها البرمجية أو الملف المنسوخ بسبب القنبلة الموقوتة(3).

وتعــرف القنــبلة المعلوماتــية بمــصطلح الــشفرة الموقــوتة Disabling Code وأكثــر مــا تبــرز فــي البــرامج المؤقتة التي تشتمل عليها الحملات الإعلانية كما هو الشأن فــي المجــلات التــي يــوزع معهــا بعــض الأســطوانات الهدية والتي تحتوى على بعض البــرامج، وهــناك أيــضا بعــض المواقــع على شبكة الإنترنت التي تشتمل على بعضا من هــذه البــرامج . كــذلك مــن الممكــن أن تظهــر فــي البرامج المؤجرة التي لا يفقد مالكها علــيها حقــوق الملكــية فهــو يقــوم بتأجيــرها فقــط، فــإذا توقف المستأجر عن دفع القيمة الايجاريــة المــتفق علــيها عــدا ذلــك إخــلالا بالعقد المبرم بين المالك والمستأجر مما يدفع بالمالــك إلــى أن يرســل لــه قنــبلة موقــوتة أو أن تكون القنبلة أصلا موجودة في البرنامج المستأجر فلا يرسل المالك ما يوقف انفجارها .

وهذا النوع من البرامج الضارة ينقسم إلى قسمين هما :

---

(1) د. جميل عبد الباقي الصغير : مذكرات في الحاسب الآلي، المرجع السابق ص 33.
(2) د. عمر محمد أبو بكر بن يونس : الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق ص371.
(3) د. عمر محمد أبو بكر بن يونس : الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق ص371-372.

1- القنبلة المنطقية Logic Bomb : وهذا النوع ينشط بمجرد حدوث واقعة معينة مثل بدأ التشغيل أو عند إنجاز أمر معين في الحاسب الآلي أو عند بدأ تشغيل برنامج معين .

ومن الأمثلة على ذلك زرع القنبلة المنطقية لتعمل لدى إضافة سجل موظف بحيث تنفجر لتمحو سجلات الموظفين الموجودة أصلا في المنشأة مثلما حصل في ولاية لوس أنجلس الأمريكية عندما تمكن أحد الأشخاص العاملين في إدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها، مما أدى إلى تخريب النظام عدة مرات[1].

2- القنبلة الزمنية Time Bomb: وهنا البرنامج ينشط في تاريخ معين محدد بالذات فهو يثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة والوقت اللازم .

ومن الأمثلة الواقعية قيام شخص يعمل بوظيفة محاسب خبير في نظم المعلومات بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة بدافع الانتقام، حيث انفجرت بعد مضي ستة أشهر من رحيله عن المنشأة وترتب على ذلك إتلاف كل البيانات المتعلقة بها[2].

خامسا: الباب الخفي Back Door :

نشأت هذه البرامج في الأصل كآلية يستخدمها المبرمجون لتضمن لهم مدخلا خاصا للأنظمة التي يقومون ببرمجتها، خاصة عندما يتسبب خطأ برمجي في التوقف التام للنظام، وفي بعض الأحيان يقومون بذلك لأسباب خبيثة أو على الأقل مشبوهة. ومع الوقت أصبحت تستخدم من قبل الهكر في الولوج الأنظمة المعلوماتية، وإختراقها.

وأنوع شفرة الباب الخفي كثيرة ومتعددة، ولكنها تجتمع في كونها تعطي ولوجا خاصا يتجاوز الإجراءات الروتينية، ورغم أن البعض يخلط بينها وبين حصان طروادة إلا أنه يمكن التفريق بينهما من حيث أن الأخير يوحي للمستخدم بأنه برنامج ذو منفعة، في حين أن برامج الباب الخفي تقوم بعملها في الخفاء[3].

---

(1) محمد أمين أحمد الشوابكة : المرجع السابق ص 240-241.
(2) محمد أمين أحمد الشوابكة: المرجع السابق ص241.
(3) محمد بن نصير محمد السرحاني: المرجع السابق ص 41.

سادسا: برمجيات ويب التفاعلية :

قـد يـسيء بعـض المبـرمجين توظـيف بعـض البـرمجيات المخصـصة لمواقع الإنتـرنت التفاعلـية والتـي تكـون عـبارة عـن ملفـات تنفيذية يتم تحميلها وتشغيلها على جهـاز المـستخدم فـور اتـصاله بالموقـع الموجـودة عليه، ومن هذه البرمجيات برمجيات جافـا وأكـتف أكـس، ورغـم أن هاتـين الوسيلتين صممتا بهدف تسهيل تفاعل زوار مواقع الإنتـرنت إلا أنـه متـى مـا تم برمجتها عن قصد بأعمال أخرى يمكنها أن تلحق بأجهزتهم الكثير من الأضرار[1].

(1) See: Oppliger, Rolf 2003:Security Technologies for the Word Wide Web. Nov. Wood , MA: Artech House.